Лабораторная работа – Настройка локальной политики безопасности

# Введение

В этой лабораторной работе вы настроите локальную политику безопасности Windows. Локальная политика безопасности Windows используется для настройки различных требований безопасности для автономных компьютеров, не входящих в домен Active Directory. Вы измените требования к паролю, включите аудит, настройте некоторые права пользователя и установите некоторые параметры безопасности. Затем вы будете использовать диспетчер событий для просмотра зарегистрированной информации.

# Рекомендуемое оборудование

* Компьютер с установленной Windows.

**Примечание**. Доступ к инструменту локальной политики безопасности немного отличается в зависимости от версии Windows. Но после того, как он будет открыт, конфигурации для остальных шагов в этой лабораторной работе будут такими же.

# Инструкции

## Ознакомьтесь с требованиями безопасности.

Клиенту необходимо иметь шесть автономных компьютеров Windows в филиале, настроенных в соответствии с политикой безопасности организации. Эти компьютеры не являются частью домена Active Directory. Политики должны быть настроены вручную на каждом компьютере.

Политика безопасности выглядит следующим образом:

* Пароли должны быть не менее 8 символов.
* Пароли необходимо менять каждые 90 дней.
* Пользователь может изменить свой пароль один раз в день.
* Пользователь должен использовать уникальный пароль не менее чем для 8 смен пароля.
* Пароль должен состоять из трех из следующих четырех элементов:
* Хотя бы один буквенный символ нижнего регистра.
* Хотя бы один альфа-символ верхнего регистра.
* Хотя бы один цифровой символ.
* По крайней мере, один символ символа.
* Пользователи блокируются от компьютера после 5 попыток ввести правильный пароль. Пользователь должен подождать 5 минут, пока счетчик просмотра не сбросится.
* Каждый параметр безопасности для политики аудита должен быть включен.
* Через 30 минут бездействия пользователь автоматически выйдет из системы. (только для Windows 8.1 и 8.0)
* Пользователи должны войти в систему, прежде чем снимать ноутбук с док-станции.
* При входе пользователям должны быть представлены следующие заголовок и текст:
* Название: **Внимание:**
* Текст: **Ваша активность отслеживается. Этот компьютер предназначен только для служебного использования.**
* Пользователи получат напоминание о смене пароля за 7 дней до истечения срока его действия.

Инструмент локальной политики безопасности Windows предоставляет гораздо больше параметров, которые выходят за рамки этого курса.

## Откройте средство локальной политики безопасности Windows.

* + 1. Чтобы получить доступ к локальной политике безопасности в Windows 10, вы можете использовать следующие два пути:

**Административные инструменты > Локальная политика безопасности**

Или, **Поиск > secpol.msc** а затем щелкните **secpol.msc**.

* + 1. Откроется окно Локальная **политика безопасности .** Эта лабораторная работа будет посвящена **политикам учетных записей** и **локальным политикам** , как показано на рисунке ниже. Остальные **настройки безопасности** выходят за рамки этого курса.

## Настройте параметры безопасности политики паролей.

Первые шесть требований политики безопасности компании настраиваются в разделе « **Политики учетных записей» инструмента «Локальная политика безопасности»** .

* + 1. Щелкните стрелку рядом с **пунктом «Политики учетных записей»** , чтобы развернуть его, а затем щелкните **«Политика паролей»** . На правой панели отображаются шесть политик со связанными с ними параметрами безопасности по умолчанию.
    2. Первая политика, **Enforce password history** , используется для установки количества уникальных паролей, которые пользователь должен ввести, прежде чем ему будет разрешено повторно использовать пароль. Согласно политике безопасности организации на шаге 1 параметр безопасности для этой политики должен быть равен **8** . Дважды щелкните **Принудительно использовать историю паролей** , чтобы открыть окно **Свойства Принудительно применять историю паролей** . Установите значение **8** .
    3. Используя требования политики безопасности на шаге 1, заполните значения, которые вы должны установить в **локальной политике безопасности** для остальных параметров безопасности **политики паролей** .

| Политика | Настройка безопасности |
| --- | --- |
| Использовать историю паролей | 8 |
| Максимальный срок действия пароля | пустой |
| Минимальный срок действия пароля | пустой |
| Минимальная длина пароля | пустой |
| Пароль должен соответствовать требованиям сложности | пустой |
| Храните пароли с помощью обратимого шифрования | Неполноценный |

**Примечание** . Параметр безопасности **«Хранить пароли с использованием обратимого шифрования»** всегда должен быть отключен. Хранение паролей с использованием обратимого шифрования по существу не отличается от хранения версий паролей в виде открытого текста. По этой причине никогда не следует включать эту политику, если только требования приложения не перевешивают необходимость защиты информации о пароле.

* + 1. Дважды щелкните каждую из политик и установите значения в соответствии с вашими записями в таблице выше.

## Настройте параметры безопасности политики блокировки учетной записи.

* + 1. Согласно политике безопасности на шаге 1, сколько раз пользователю разрешено пытаться войти в систему, прежде чем его учетная запись будет заблокирована?

5 попыток

* + 1. Как долго пользователь должен ждать, прежде чем попытаться снова войти в систему?

5 минут

* + 1. Используйте параметры безопасности **политики блокировки учетных записей** в **локальной политике безопасности** , чтобы настроить требования политики.

**Подсказка** : сначала вам нужно настроить **порог блокировки учетной записи** .

## Настройте параметры безопасности политики аудита.

* + 1. В «Локальной политике безопасности» разверните меню «Локальные политики» и нажмите «Политика аудита».
    2. Дважды щелкните **Аудит событий входа в учетную запись** , чтобы открыть окно **Свойства** . Щелкните вкладку **Объяснение** , чтобы узнать об этом параметре безопасности.
    3. Перейдите на вкладку **«Локальные параметры безопасности»** и установите флажки « **Успех** » и **«Сбой»** . Нажмите **OK** , чтобы закрыть окно **свойств** и применить настройки безопасности.
    4. Продолжайте изменять остальные параметры безопасности **политики аудита** . Нажмите вкладку **«Объяснение»** для каждого и прочитайте, что он делает. Установите флажки **«Успех»** и **«Неудача» в каждом окне «Свойства»** .

## Настройте дополнительные параметры безопасности локальных политик.

* + 1. В локальной политике безопасности щелкните «Назначение прав пользователя» в разделе «Локальные политики», чтобы просмотреть параметры безопасности.
    2. Хотя ни один из параметров безопасности не нужно изменять для соответствия требованиям политики безопасности, потратьте некоторое время на просмотр параметров по умолчанию.

#### Вопрос:

Есть ли какие-то, которые вы бы порекомендовали изменить? Почему?

Разрешить вход в систему через службу удалённых рабочих столов, только для администраторов или ни для кого – для запрета НСД по сети

* + 1. В локальной политике безопасности нажмите «Параметры безопасности» в разделе «Локальные политики», чтобы просмотреть параметры безопасности.
    2. Что касается остальных требований политики безопасности на шаге 1, перечислите значения политики и параметров безопасности, которые необходимо изменить в **параметрах безопасности,** в таблице ниже. Первый сделан для тебя.

| Политика | Настройка безопасности |
| --- | --- |
| Интерактивный вход: предел бездействия компьютера | 1800 секунд |
| пустой | пустой |
| пустой | пустой |
| пустой | пустой |
| пустой | пустой |

## Проверьте параметры безопасности политики паролей.

Проверьте параметры безопасности политики паролей, попытавшись изменить пароль. Попробуйте новый пароль, который не соответствует требованиям по длине или сложности.

**Панель управления > Учетные записи пользователей > Внесите изменения в мою учетную запись в настройках ПК > Параметры входа** и нажмите **Изменить** в разделе **Пароль** .

Вам должно быть представлено сообщение о том, что ваш новый пароль не соответствует требованиям политики паролей.

## Экспорт и импорт параметров политики безопасности.

У заказчика есть еще 5 автономных компьютеров, которые должны соответствовать тем же требованиям политики безопасности. Вместо ручной настройки параметров каждого компьютера экспортируйте параметры на этот компьютер.

* + 1. В строке меню локальной политики безопасности нажмите «Действие» > «Экспортировать политику...».
    2. Выберите имя для **. inf** и сохраните его в любом месте по вашему выбору.
    3. Скопируйте политику безопасности **. инф** файл на флешку. Отнесите флешку на другой компьютер. Вставьте флэш-накопитель, откройте « **Локальная политика безопасности»** и нажмите **«Действие» > «Импортировать политику».** Найдите файл **. inf** на флэш-накопителе и откройте его, чтобы применить политику безопасности к новому компьютеру.

Конец документа